This page describes how to create, modify, and delete VPC networks. This page assumes that you are familiar with the characteristics of VPC networks as described in the VPC Network Overview (/vpc/docs/vpc). Networks and subnets are different resources (/vpc/docs/vpc#vpc_networks_and_subnets) in Google Cloud.

You can choose to create an auto mode or custom mode VPC network. Each new network that you create must have a unique name within the same project.

Auto mode (/vpc/docs/vpc#subnet-ranges) networks create one subnet (/vpc/docs/vpc#vpc_networks_and_subnets) in each Google Cloud region automatically when you create the network. As new regions become available, new subnets in those regions are automatically added to the auto mode network. IP ranges for the automatically created subnets come from a predetermined set of ranges (/vpc/docs/vpc#ip-ranges). All auto mode networks use the same set of IP ranges.

:ant: Read the considerations for auto mode networks (/vpc/docs/vpc#auto-mode-considerations) before you creat
oduction use. Production networks should be planned in advance, and custom mode networks are better suited for m
:tion use cases.

For custom mode VPC networks, create a network, then create the subnets that you want within a region. You do not have to specify subnets for all regions right away, or even at all, but you cannot create instances in a region that has no subnet defined.

You can create subnets when you create the network, or you can add subnets (#add-subnets) later.

After you create a network, create firewall rules (/vpc/docs/using-firewalls) to allow or deny traffic between resources in the network, such as communication between VM instances. You also use firewall rules to control what traffic leaves or enters the VPC network to or from the internet.

View the VPC and legacy networks in your project. For VPC networks, you can view information about their subnets and their subnet creation mode.

You must follow these rules when creating or editing a subnet:

- Within a project, a subnet cannot have the same name as a VPC network unless it is a member of that network. Within a project, subnets in the same region must have unique names. For example, a network named `production` can have multiple subnets also named `production` as long as each of those subnets is in a unique region.
- You cannot change the name or region of a subnet after you have created it. However, you can delete a subnet and replace it, as long as no resources are using it.
- Each subnet must have a primary range, and, optionally, one or more secondary ranges for alias IP (/vpc/docs/alias-ip). The per network limits (/vpc/docs/quota#per_network) describe the maximum number of secondary ranges that you can define for each subnet. Primary and secondary IP ranges must be RFC 1918 (https://tools.ietf.org/html/rfc1918) addresses.
    - Within a VPC network, all primary and secondary IP ranges must be unique, but they do **not** need to be contiguous. For example, the primary range of a subnet can be `10.0.0.0/24` while the primary range of another subnet in the same network can be `192.168.0.0/16`.
    - The primary IP range for the subnet can be expanded (#expand-subnet), but not replaced or shrunk, after the subnet has been created.
    - You can remove and replace a subnet's secondary IP address range only if no instances are using that range.
    - The minimum primary or secondary range size is eight IP addresses. In other words, the longest subnet mask you can use is `/29`.
- Primary and secondary ranges for subnets **cannot** overlap with any allocated range (/vpc/docs/private-access-options), any primary or secondary range of another subnet in the same network, or any IP ranges of subnets in peered networks (/vpc/docs/vpc-peering).
- Google Cloud creates corresponding subnet routes (/vpc/docs/routes#subnet-routes) for both primary and secondary IP ranges. Subnet routes, and therefore subnet IP ranges, must have the most specific IP ranges by definition.
    - Primary and secondary ranges can't conflict with on-premises IP ranges if you have connected your VPC network to another network with Cloud VPN (/vpn/docs/concepts/overview), Dedicated Interconnect

(/interconnect/docs/how-to/choose-type#dedicated), or Partner Interconnect (/interconnect/docs/how-to/choose-type#partner).

- IP ranges for all subnets must be unique among VPC networks that are connected to one another by VPC Network Peering.
- Subnet IP ranges cannot conflict with destinations for static routes (/vpc/docs/routes#static_routes).
- Avoid using IP addresses from the `10.128.0.0/9` block for a subnet's primary or secondary IP ranges. Automatically created subnets in auto mode networks (/vpc/docs/vpc#ip-ranges) use IP addresses from this block. If you use IP addresses in the `10.128.0.0/9` block, you will not be able to connect your network to an auto mode VPC network using VPC Peering or with Cloud VPN tunnels.

You can see all the subnets that exist for a project.

You can view details of an existing subnet, such as its primary IP range, any secondary IP ranges, and its region, by following the steps in this section.

When you create a subnet, you set a name, a region, and at least a primary IP address range according to the subnet rules (#subnet-rules).

Use the following directions to delete a manually created subnet. Before you can delete a subnet, you must delete all resources that use it. For example, you need to delete VMs (/compute/docs/instances/stopping-or-deleting-an-instance#delete_an_instance), reserved internal IP addresses, internal forwarding rules, and Cloud NAT gateways that use the subnet.

For auto mode networks, you **cannot** delete any of the automatically created subnets. However, you can convert an a network to a custom mode network (#switch-network-mode) and then delete any unused automatically created sub

You can expand the primary IP range of an existing subnet by modifying its subnet mask, setting the prefix length to a *smaller* number. The proposed new primary IP range of the subnet must follow the subnet rules (#subnet-rules).

When expanding the IP range of an automatically created subnet in an auto mode network (or in a custom mode network that was previously an auto mode network), the broadest prefix (subnet mask) you can use is `/16`. Any prefix broader than `/16` would conflict with the primary IP ranges of the other automatically created subnets (/vpc/docs/vpc#ip-ranges).

n: Expanding the primary IP range of a subnet cannot be undone. You cannot shrink the primary IP range of a subne
d primary IP ranges conservatively; you can always expand them again. Consider IP address space in any networks
your VPC network is or will be connected before you expand a subnet's primary IP range.

You can add secondary IP ranges to subnets, or you can remove any secondary range as long as no resources are using IP addresses in it.

You can convert an auto mode network to a custom mode network using this procedure. Review the considerations for auto mode networks (/vpc/docs/vpc#auto-mode-considerations) for background information about reasons why you might want to do this.

Converting an auto mode network to a custom mode network **preserves** all of its automatically created subnets and any subnets you have added. Subnet names and IP ranges are not changed.

:ant: You cannot convert a custom mode network to an auto mode network. Conversion from auto to custom mode ay process. Auto mode networks that have been converted to custom mode operate as if they had been created in cu

After you convert an auto mode network to custom mode, you must review all API calls and `gcloud` commands that implicitly reference any subnet that was automatically created while the network was in auto mode. API calls and commands will need to be modified so that they reference the subnet explicitly. For `gcloud` commands that have a subnet specification flag (`--subnet`), that flag is required to reference subnets in a custom mode network.

Each VPC network has an associated dynamic routing mode that controls the behavior of Cloud Routers in the network. Refer to dynamic routing mode (/vpc/docs/vpc#routing_for_hybrid_networks) section in the *VPC Network Overview* page to understand how each mode affects how Cloud Routers share routes and apply learned routes.

›n: Changing the dynamic routing mode has the potential to interrupt traffic within the network, or enable or disable r
‹pected ways. Carefully review the role of each Cloud Router before changing the dynamic routing mode.

If a network is not being used, you can delete it. Before you can delete a network, you must delete all resources in all of its subnets, and all resources that reference the network. Resources that reference the network include Cloud VPN gateways, Cloud Routers, firewall rules, and custom static routes.

You can enable logging of network flows to and from VMs. See Using VPC Flow Logs (/vpc/docs/using-flow-logs) for instructions.

You can enable logging for firewall rules to see which rules allowed or blocked which traffic. See Using Firewall Rules Logging (/vpc/docs/using-firewall-rules-logging) for instructions.

- See Routes Overview (/vpc/docs/routes) for information on routes.
- See Firewall Rules Overview (/vpc/docs/firewalls) for information on firewall rules.
- See Advanced VPC Concepts (/vpc/docs/advanced-vpc) for deeper details on VPC networking.